ENERGY SHIELD

ENERGYSHIELD PROJECT

Project progress and achivements
CPS4CIP 2021, 8th of October 2021

Facilitator: Otilia Bularca, Project Manager, SIMAVI

AGENDA

01 ABOUT ENERGYSHIELD PROJECT

02 TOOLS

03 PILOTS DEPLOYED

04 IMPACT & LESSONS LEARNED

ENERGY SHIELD

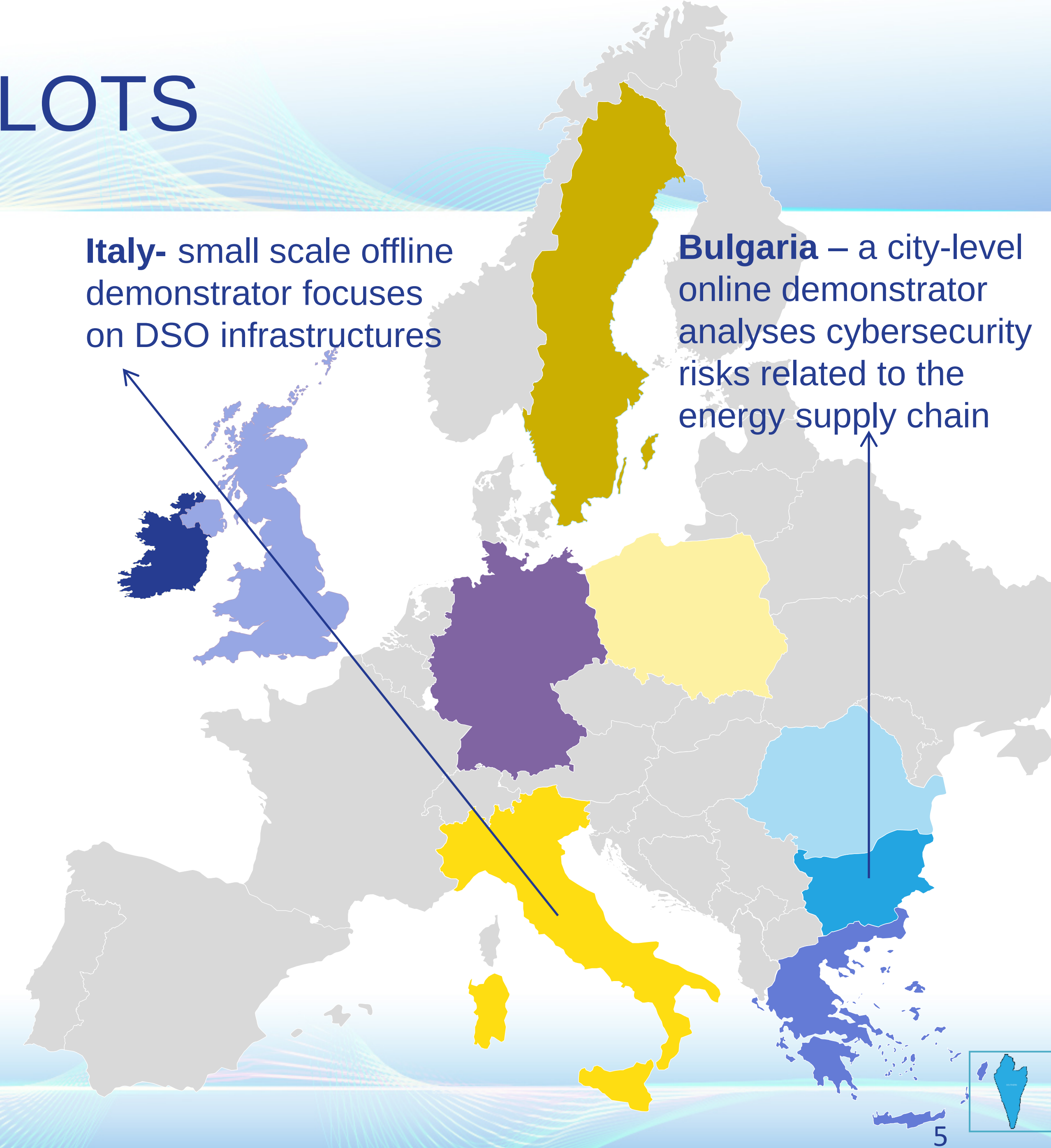
ABOUT THE PROJECT

ENERGYSHIELD PROJECT IN A NUTSHELL

- Title: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures
- Type of Action: Innovation Action
- Topic: SU-DS04-2018-2020
  - Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
- Goal
  - EnergyShield captures the needs of Electrical Power and Energy System (EPES) operators and combines the latest technologies for vulnerability assessment, supervision and protection to draft a defensive toolkit.
- Start date: 1st of July 2019
- Duration: 36 months
- Grant: € 7,421,437.38

CONSORTIUM AND PILOTS

Romania:	Software Imagination & Vision
Germany:	PSI Software AG
Israel :	SI-GA Data Security (2014) LTD
	L7 Defense LTD
Sweden:	foreseeti AB Kungliga Tekniska Hoegskolan
UK:	Tech Inspire LTD City University Of London
Ireland:	Konnekt Able Technologies
Greece:	National Technical University Of Athens
Bulgaria:	Software Company EOOD Kogen Zagore EOOD MVETS Lenishta OOD Elektroenergien Sistemen Operator EAD CEZ Distribution Bulgaria AD MIG 23 LTD DIL DIEL
Italy	IREN SPA



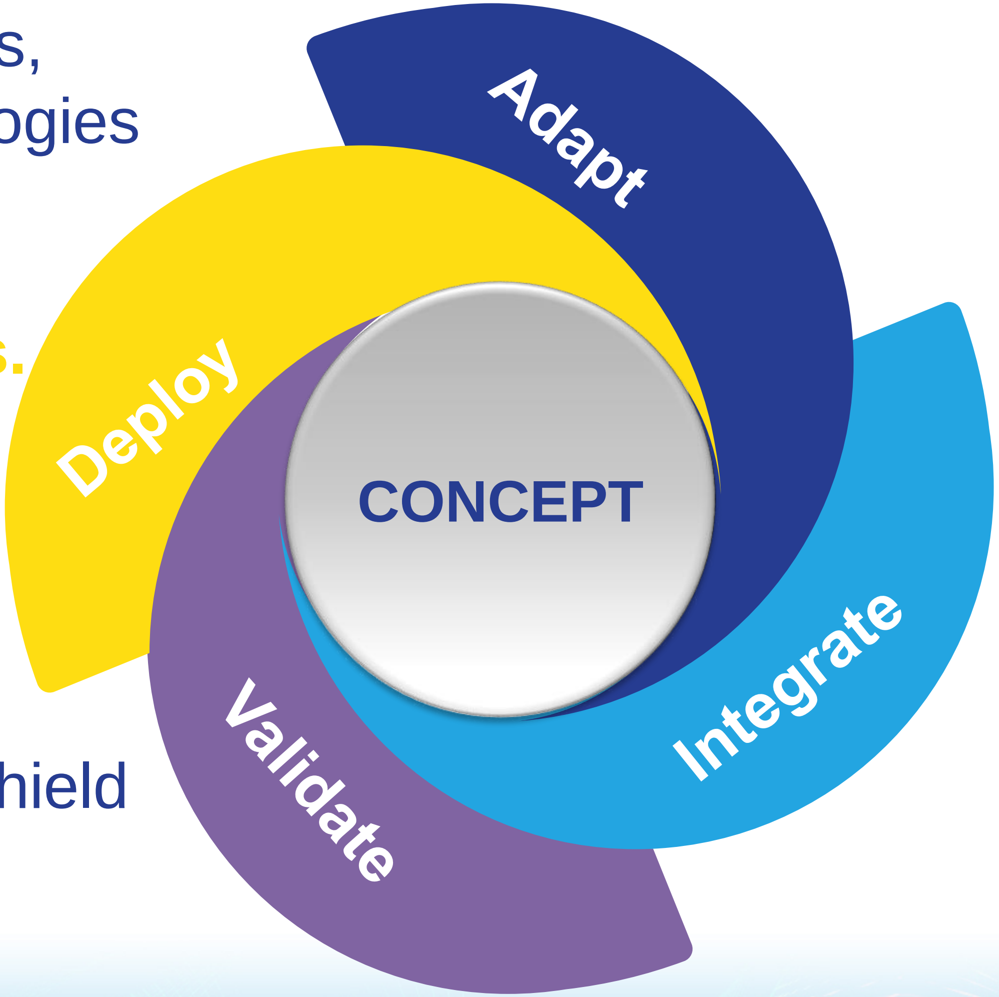
Italy- small scale offline demonstrator focuses on DSO infrastructures

Bulgaria – a city-level online demonstrator analyses cybersecurity risks related to the energy supply chain

CONCEPT AND OBJECTIVES

Deploy best practices, guidelines, methodologies and encourage the adoption of EnergyShield **results.**

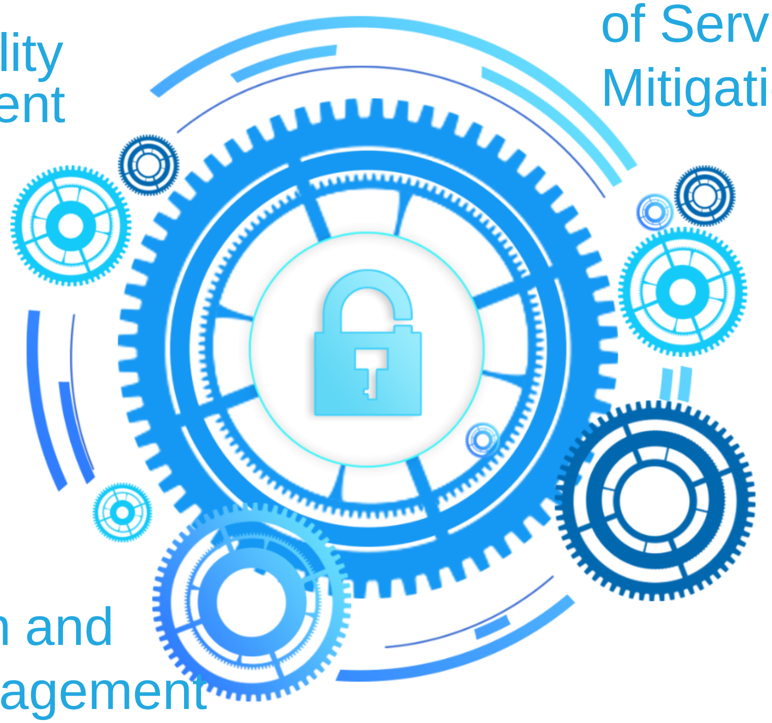
Adapt and improve available **tools** to support Electrical Power and Energy System (EPES) in fighting against cyber attacks.



Validate the practical value of the EnergyShield **toolkit** with EPES stakeholders.

Integrate the cybersecurity tools in **a holistic solution** with assessment, monitoring, protection and learning capabilities.

ENERGYSHIELD TOOLS



Vulnerability Assessment

Distributed Denial of Service Mitigation

Security Behaviour Analysis

Anomaly Detection

Security Information and Event Management

Small scale attacks

- Targeting specific organization
- Meant to prevent them from conducting business normally
- *e.g. Distributed Denial of Service, ransomware*

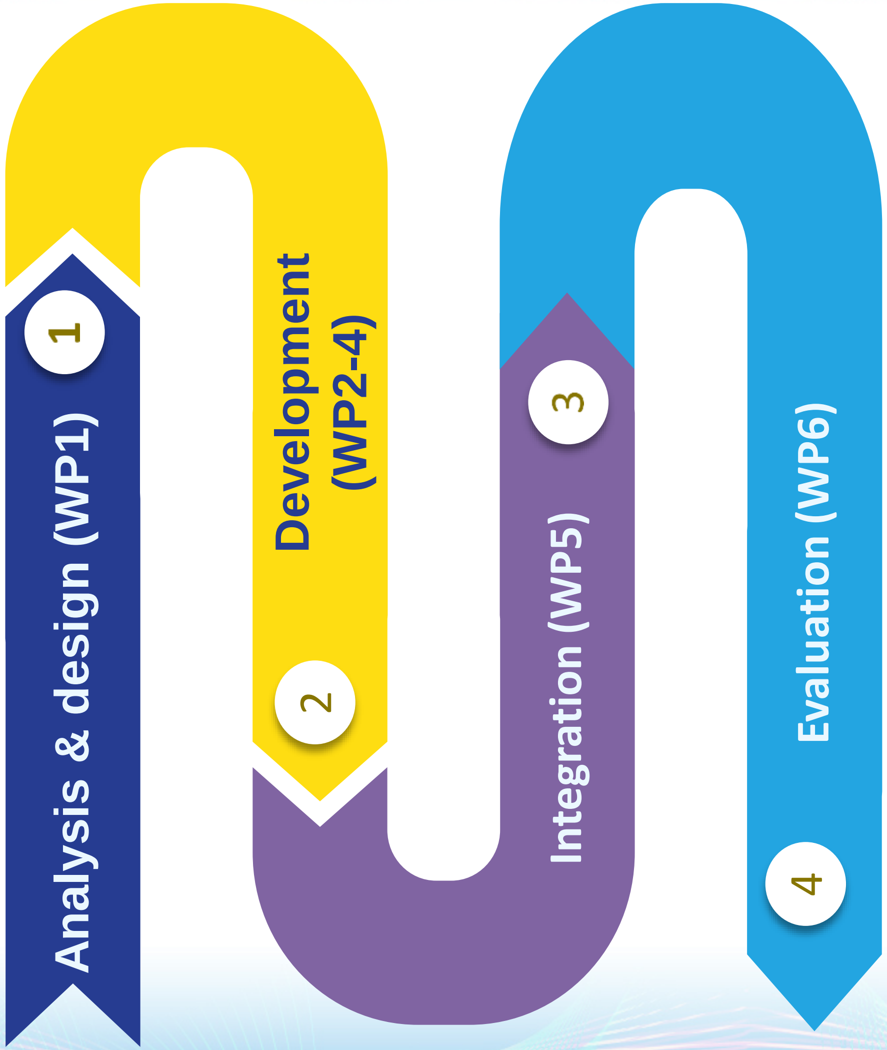
Large scale attacks

- Targeting the entire EPES value chain
- Meant to take down the energy supply services at regional or country level
- *e.g. malware deployment, man-in-the-middle*

TECHNICAL ACTIVITIES PROGRESS

- Analysis
- Architecture
- Functional Requirements
- Non-Functional Requirements

- Tools roadmap
- Tools release plan
- Demonstrators timeplan



- Integration plan
- Deployment plans
- Test plan
- Toolkit demo release timeline

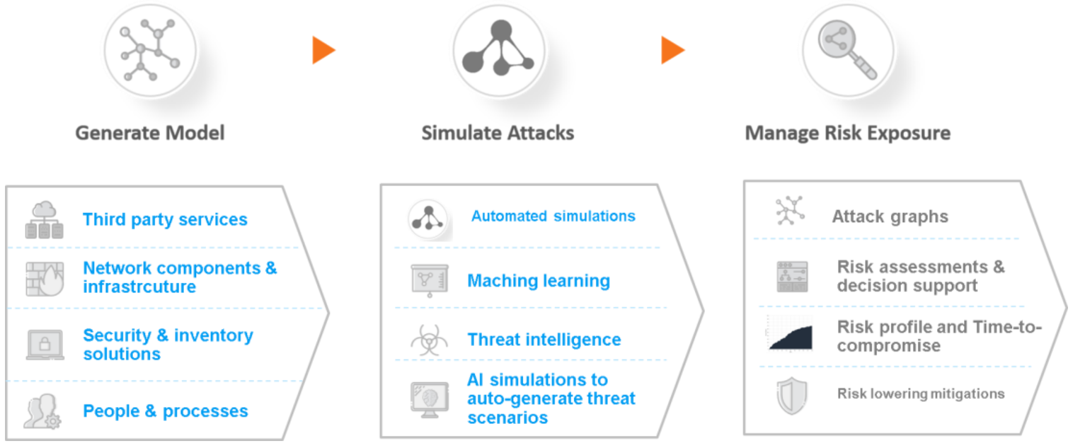
- User needs
- Tools evaluation
- On-site deployment
- Piloting
- Evaluation

ENERGY SHIELD

TOOLS

VULNERABILITY ASSESSMENT TOOL

- Tool contributors
  - Leading partner: FOR
  - Contributing partners: **KTH**, PSI, SIMAVI
- Tool features
  - *Threat modelling & Attack Simulations*
    - Analyze cyber resilience in complex systems
    - Bayesian probability networks, Monte Carlo simulations and k-means clustering
  - *Operates on a model – a cyber “digital twin”*
    - Non-intrusive, risk-free
    - Exactness determined by the threat modelling “language” and quality of model
    - Cyber threats are automatically derived from the structural system model
  - *“The language” epesLang*
    - Codifies the cyber-characteristics of ICS and the electrical energy sector systems
    - Based on Meta Attack Language (https://mal-lang.org)
- TRL – Started on 7, targeting 8 (9 after project end)



Generate Model

Third party services

Network components & infrastrcuture

Security & inventory solutions

People & processes

Simulate Attacks

Automated simulations

Maching learning

Threat intelligence

AI simulations to auto-generate threat scenarios

Manage Risk Exposure

Attack graphs

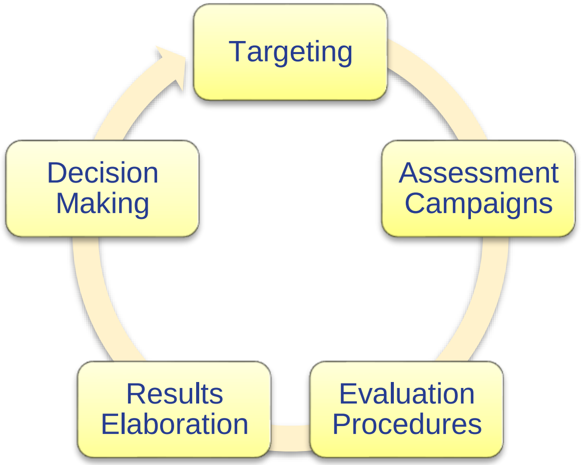
Risk assessments & decision support

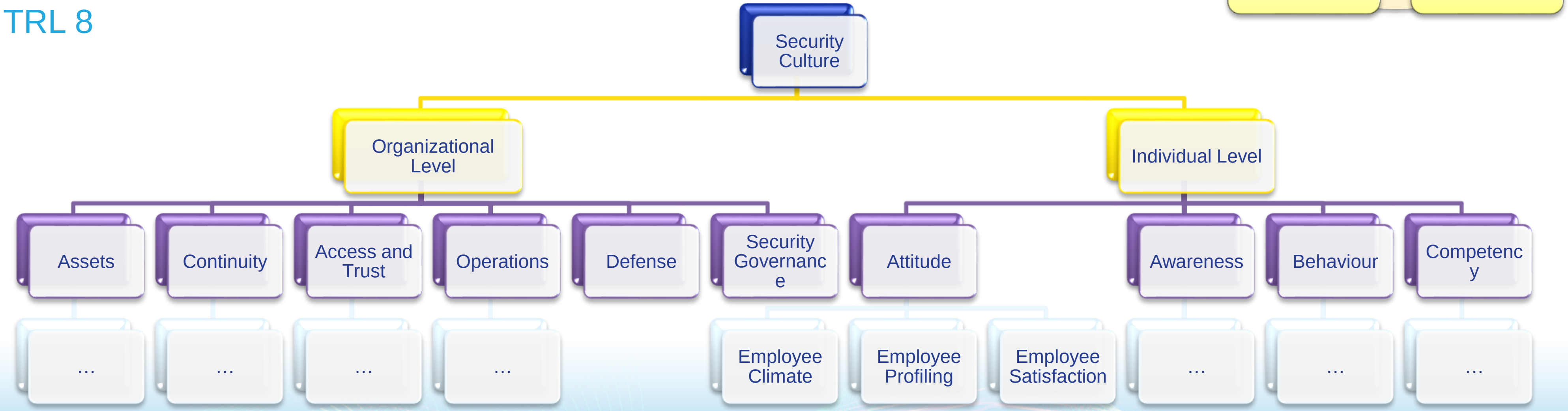
Risk profile and Time-to-compromise

Risk lowering mitigations

SECURITY BEHAVIOR ANALYSIS TOOL (I)

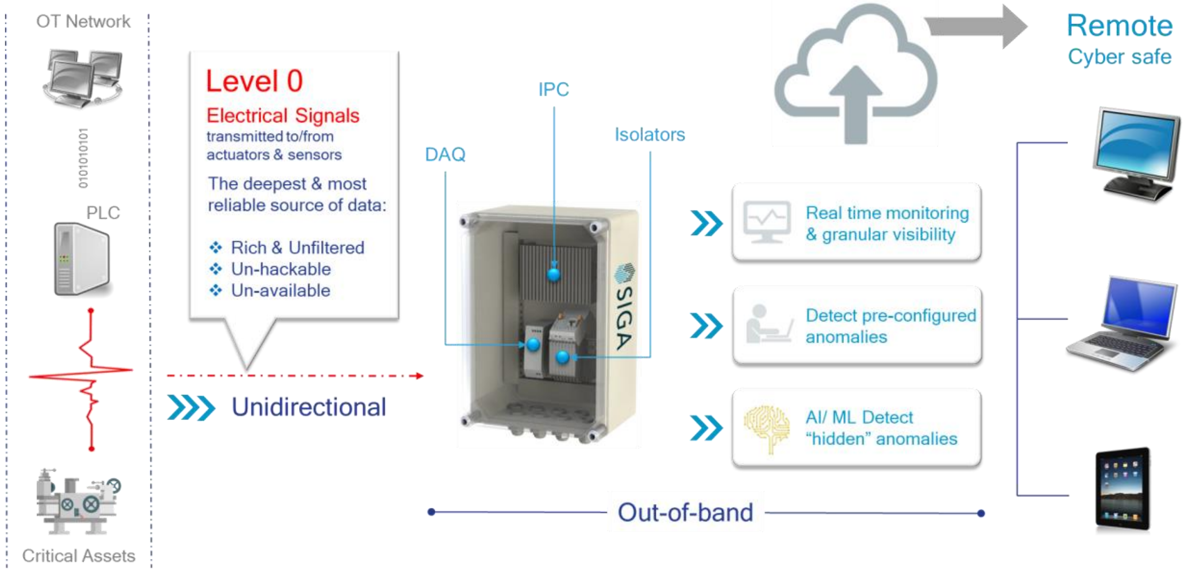
- Tool contributors
  - Leading partner: **NTUA**
  - Contributing partners: FOR, KTH, SC, IREN
- Tool features
  - Founded on a cyber-security culture model: **levels, dimensions** and **domains**
  - Evaluation methodology: **campaigns** and **self-assessment** possibilities
  - **Socio-cultural behaviour mapping to specific cyber-threats**
  - **Decision-making insights and recommendations towards security culture improvement**
  - **Assistance into planning and implementing security culture training programs**
  - Open, highly **customizable** and **interoperable** with third-party components
- TRL 4 → TRL 8





ANOMALY DETECTION TOOL

- Tool contributors
  - Leading partner: SIGA
  - Contributing partners: SC, IREN, SIMAVI
- Tool features
  - SIGA's topology & architecture
  - Improved anomaly detection algorithms
  - Extended user's understanding of anomalies
  - Extended variety of sources of process data
  - Higher detection rate and lower or identical false-positive rate compared to existing algorithms
  - By developing the alert text to be set by the specific anomaly
  - Taking data from higher levels (agent on PLC, Communication device etc.)
- TRL -started at 7 and is targeting 8


OT Network
0101010101
PLC
Critical Assets
Level 0
Electrical Signals
transmitted to/from actuators & sensors
The deepest & most reliable source of data:
❖ Rich & Unfiltered
❖ Un-hackable
❖ Un-available
Unidirectional
DAQ
IPC
Isolators
SIGA
Real time monitoring & granular visibility
Detect pre-configured anomalies
AI/ ML Detect "hidden" anomalies
Out-of-band
Remote
Cyber safe

DISTRIBUTED DENIAL OF SERVICE MITIGATION TOOL

- Tool contributors
  - Leading partner: L7 Defense
  - Contributing partners: CITY, SC and SIMAVI
- Objective
  - Improve the Real time DDoS mitigation for Energy IT
  - Adjust L7 Defense Ammune AI to secure Smart Grids from DDoS attacks
  - Ensure critical business energy operation continuity
    - Outage prevention. DDoSM uses ML to detect and mitigate application-layer DDoSM attack on the communication infrastructure
    - Disruption attacks prevention. AD can detect anomalies at the OT layer and consequently protect systems against MITM/replay attacks on control infrastructure
    - AD & DDoSM can actively defend infrastructures against DDoS or malware-based attacks
- TRL 6 → TRL 8

Innate Immune Theory

- **It defines a novel unsupervised learning approach**
- **It automatically detects unknown automated threats**
- **It is made for highly controlled and precise mitigation process**

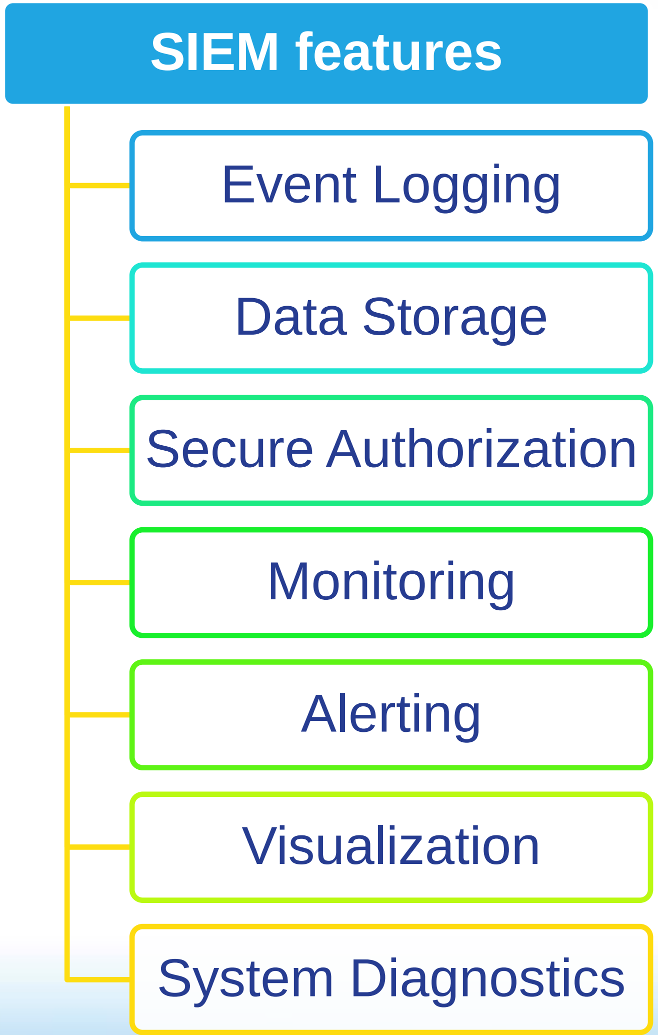
L7 Defense Ammune™ API Security Solution Origins Are In Nature

"Innate" Immune Model

1. It automatically detects unknown automated threats
2. It is made for highly controlled & precise mitigation process
3. Autonomous system - no human intervention required
4. Installation is straight forward - Plug & Play
5. No pre-training required, protection is immediately activated

SIEM TOOL – CONCEPT AND OBJECTIVES

- Tool contributors
  - Leading partner: KT
  - Contributing partners: SIGA, FOR, L7D, TEC, NTUA, SC
- Tool objectives
  - Adapt and customise an open source SIEM tool able to:
    - Detect suspicious activity from multiple sources and endpoints
    - Interact with the other EnergyShield tools and components
  - SIEM combines security information management (SIM) with security event management (SEM) forming a single collaborative security management system.
  - Information(logs, events, metrics) from multiple sources and endpoints is collected and analyzed using rules-based protocols
  - Detect suspicious activity in an efficient and timely manner with the help of features
- TRL 8
- Concept tools to be integrated within SIEM
  - Homomorphic encryption
  - Automated forensic tool

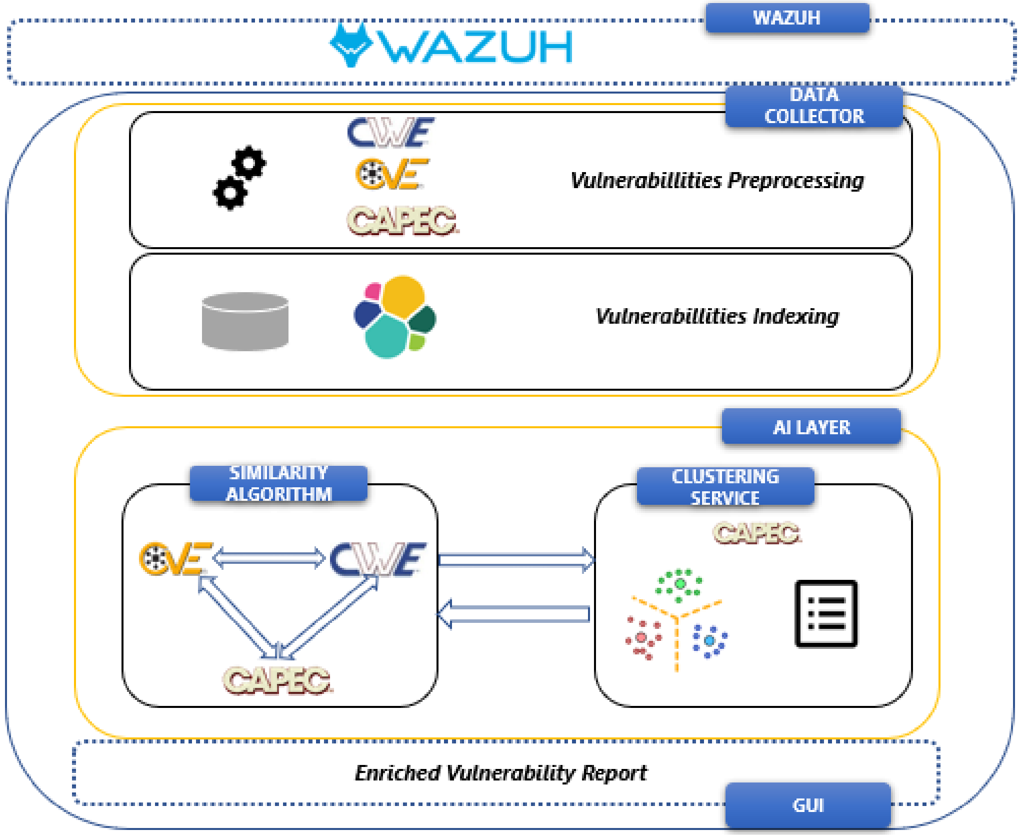


SIEM features

- Event Logging
- Data Storage
- Secure Authorization
- Monitoring
- Alerting
- Visualization
- System Diagnostics

AUTOMATED FORENSIC TOOL

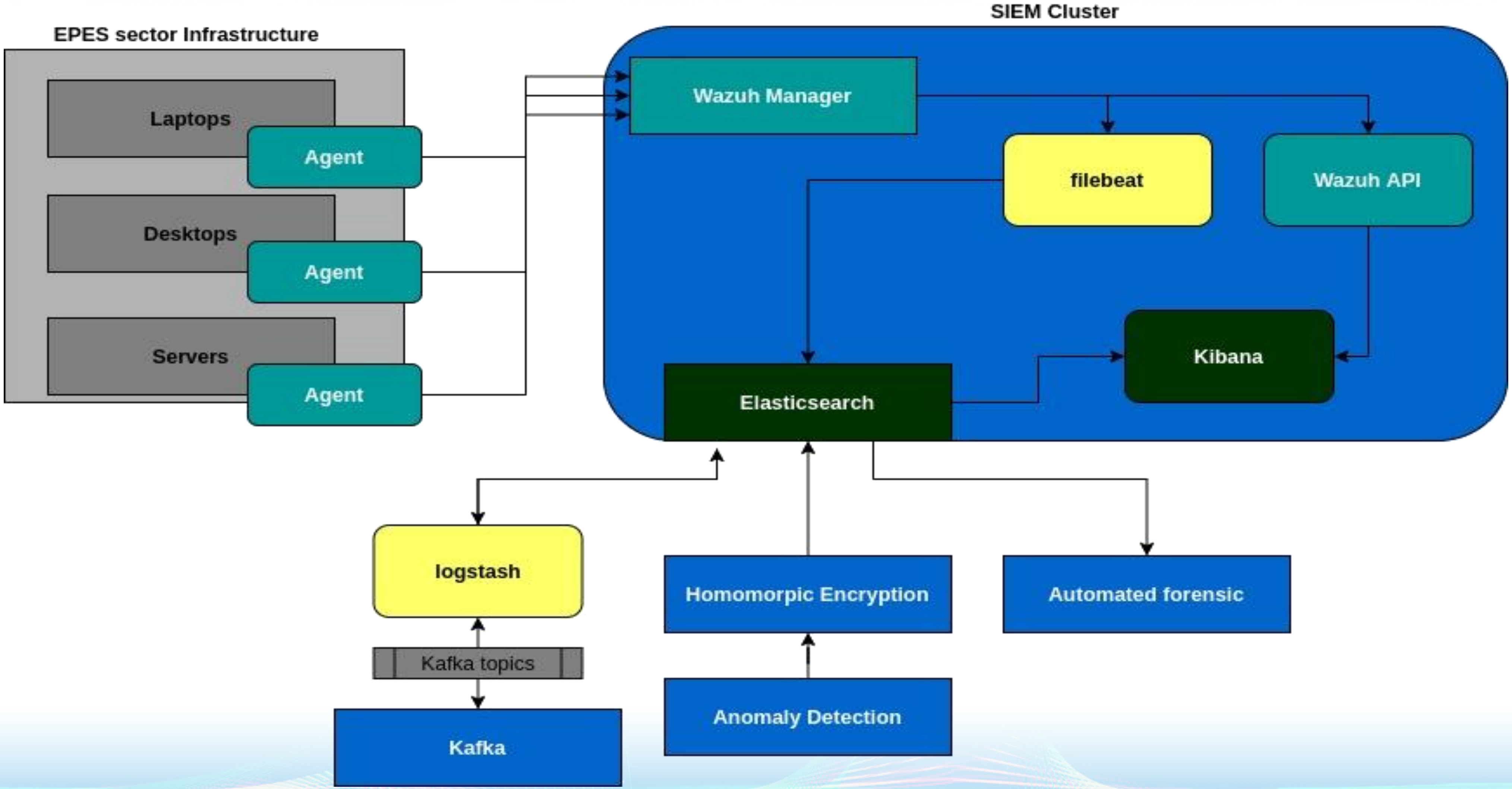
- The objective of the Automated Forensic Module is to provide richer information for the security threat events detected by the EnergyShield SIEM tool by extracting information from external vulnerability databases
  - CVE - Common Vulnerabilities and Exposures
  - NVD - U.S. National Vulnerability Database
  - CWE - Common Weakness Enumeration
  - CAPEC - Common Attack Pattern Enumeration and Classification
  - ATT&CK – A globally-accessible tactics and techniques dictionary by MITRE Corporation
  - OWASP - Open Web Application Security Platform
  - WASC - Web Application Security Consortium
- Intelligent rules are used to discover hidden patterns on vulnerabilities
- TRL 4 -> TRL 5



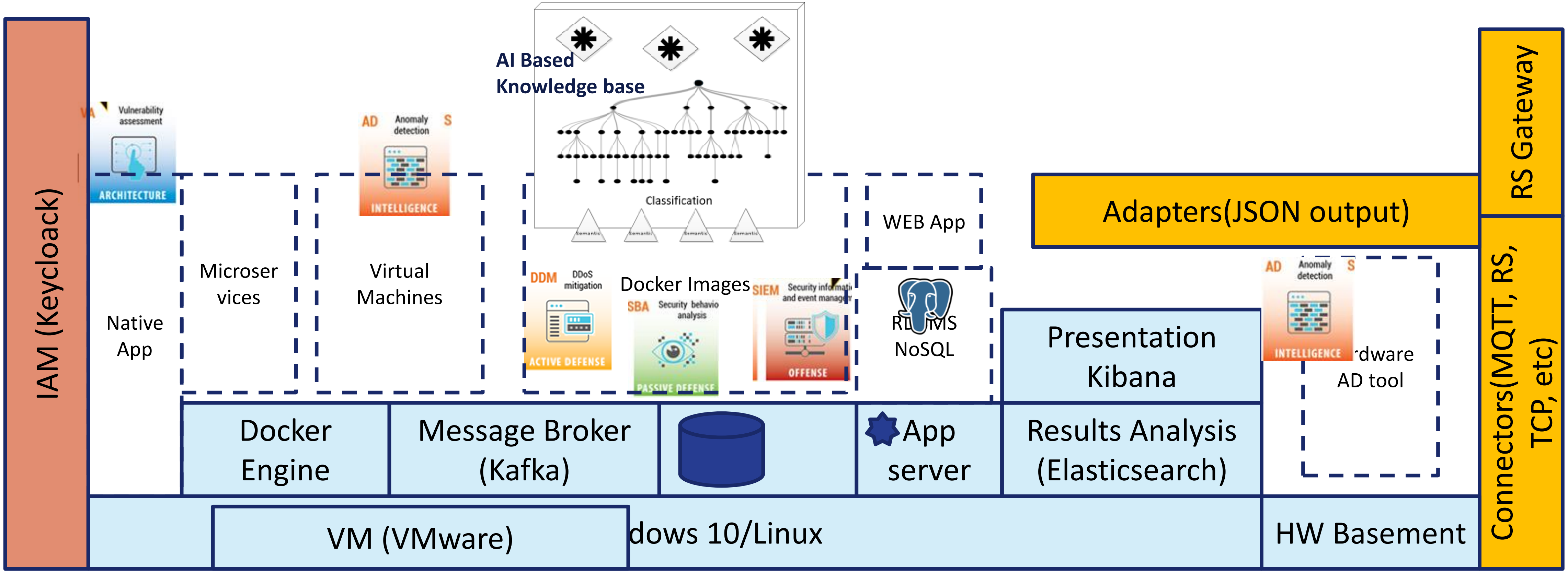
HOMOMORPHIC ENCRYPTION TOOL

- Status quo
  - Private data needs to be secured
  - Techniques used: pseudonymisation and anonymisation
- Improvement proposal
  - Homomorphic Encryption (HE) tool – data in ciphertext can be analyzed and worked with
- Challenges
  - HE is that they often increase the ‘noise: slows down processing speed, can make the decryption operation worthless.
- Solution:
  - automated framework which reduces the noise of HE operations
  - develop a searchable HE encryption tool based on Rivest-Shamir-Adleman (RSA).

SIEM INTEGRATION



ENERGYSHIELD TOOLKIT ORGANIZATION



IAM (Keycloack)

Native App

Microser vices

Virtual Machines

AI Based Knowledge base

Docker Images

WEB App

RDBMS NoSQL

Adapters(JSON output)

RS Gateway

Presentation Kibana

rdware AD tool

Docker Engine

Message Broker (Kafka)

App server

Results Analysis (Elasticsearch)

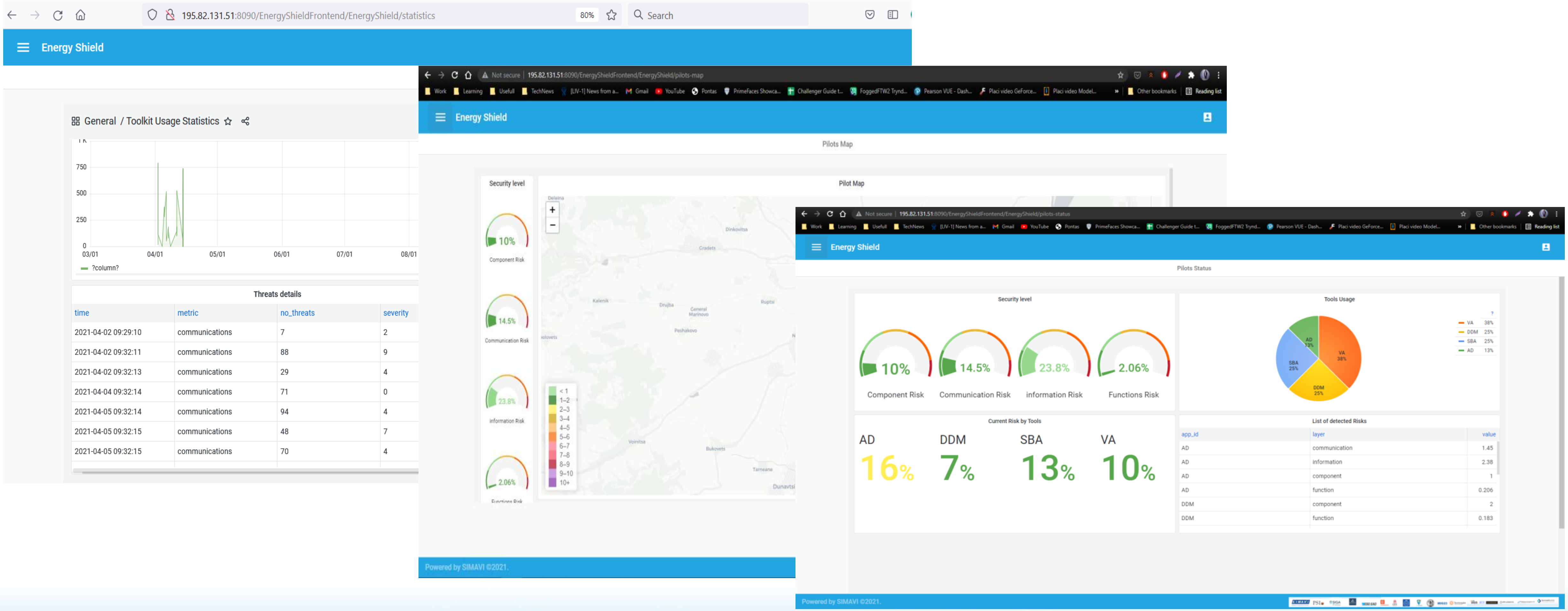
VM (VMware)

dows 10/Linux

HW Basement

Connectors(MQTT, RS, TCP, etc)

ENERGYSHIELD PORTAL



195.82.131.51:8090/EnergyShieldFrontend/EnergyShield/statistics

Energy Shield

General / Toolkit Usage Statistics

Threats details

time	metric	no_threats	severity
2021-04-02 09:29:10	communications	7	2
2021-04-02 09:32:11	communications	88	9
2021-04-02 09:32:13	communications	29	4
2021-04-04 09:32:14	communications	71	0
2021-04-05 09:32:14	communications	94	4
2021-04-05 09:32:15	communications	48	7
2021-04-05 09:32:15	communications	70	4

195.82.131.51:8090/EnergyShieldFrontend/EnergyShield/pilots-map

Energy Shield

Pilots Map

Security level

Pilot Map

Powered by SIMAVI ©2021.

195.82.131.51:8090/EnergyShieldFrontend/EnergyShield/pilots-status

Energy Shield

Pilots Status

Security level

Tools Usage

Current Risk by Tools

AD	DDM	SBA	VA
16%	7%	13%	10%

List of detected Risks

app_id	layer	value
AD	communication	1.45
AD	information	2.38
AD	component	1
AD	function	0.206
DDM	component	2
DDM	function	0.183

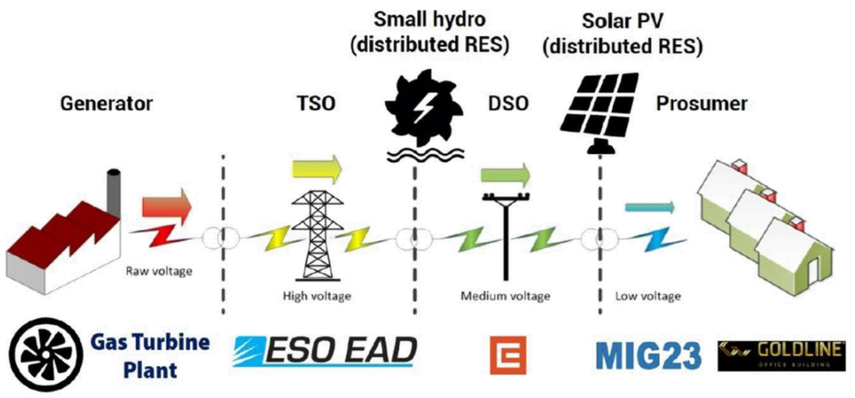
Powered by SIMAVI ©2021.

ENERGY SHIELD

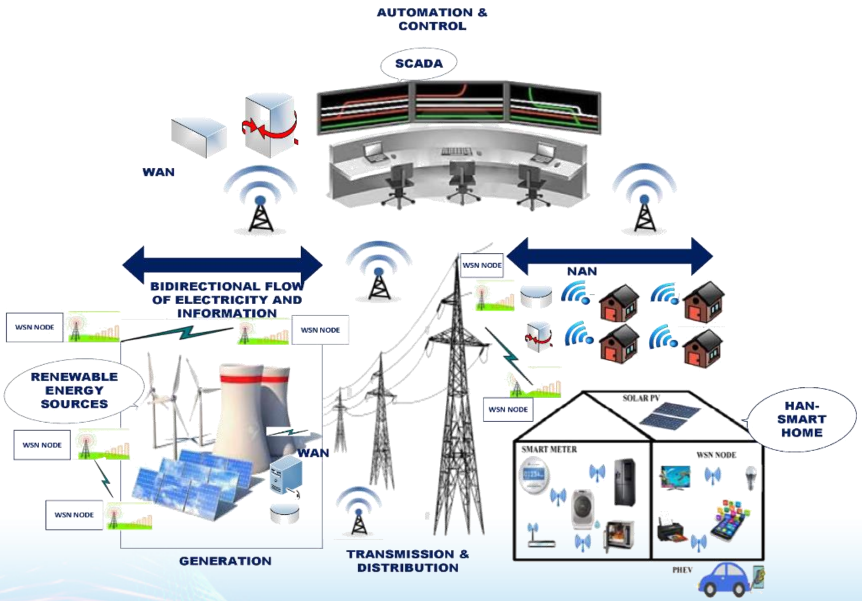
PILOTS DEPLOYED

BULGARIAN PILOT IN A NUTSHELL

- Aim
  - to evaluate the most effective solutions to prevent, detect, and mitigate malicious cyber-attacks
- Scenarios
  - Attacks on Substation Infrastructure
  - Attacks on Consumer / Prosumer networks points
- Infrastructure
  - one primary substation (operated by ESO),
  - secondary substations (operated by CEZ),
  - gas-turbine plant (CoTTP)
  - hydro generation plant (RES),
  - prosumer GOLD (producer and consumer)
  - regular CEZ residential consumers
  - In the Bulgarian electricity system, there is a SCADA system installed and operated in the various substations connecting the 400,220,110 kV lines network.
  - PLC/RTUs and measurement systems (energy meters, PMUs, DLR sensors) are interconnected by using the DNP3/IEC60870-5/IEC61850 protocols.
- Tools proposed and TRL progress
  - Vulnerability assessment module [TRL 7 to 8]
  - Security behaviour analysis module [TRL 4 to 8]
  - Anomaly detection module [TRL 7 to 8]
  - DDoS mitigation module [TRL 6 to 8]
  - Security information and event management module [TRL 6 to 8]

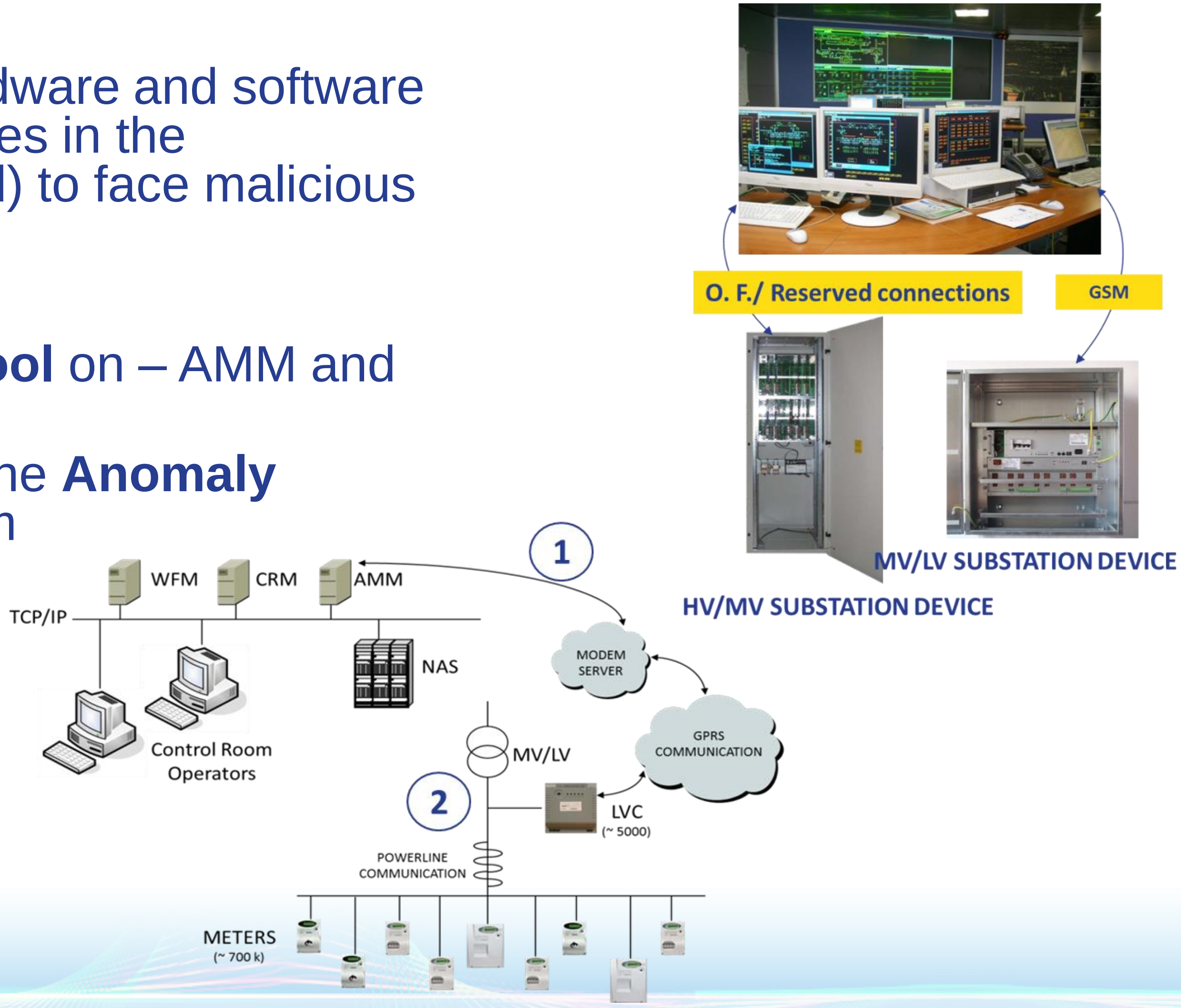


EPES value chain



ITALIAN PILOT IN A NUTSHELL

- Aim
  - to evaluate the most effective solutions (hardware and software solutions, organizational approaches, changes in the procedures and qualified the staff in this field) to face malicious cyber-attacks.
- Scenarios
  - Testing the **Security Behaviour Analysis tool** on – AMM and Network remote control system
  - Perform a feasibility study on integration of the **Anomaly detection tool** on its specific SCADA system
- Infrastructure
  - HV/MV Remote control system and SCADA
    - Network monitoring
    - Fault/outage detection
    - Emergency operations
  - Smart metering infrastructure



ENERGY SHIELD

IMPACT & LESSONS LEARNED

EXPECTED IMPACT & CHALLENGES

- EnergyShield project addresses
  - the implementation gap between research projects and industrial applications (NISD)
  - The particularities of cybersecurity in energy sector *[EC Recommendation on cybersecurity in energy sector SWD(2019) 1240]*
    - real-time requirements (certain processes cannot be delayed)
    - cascading effect (compromise can trigger back-outs)
    - technology mix (risk form legacy components)
- End users: EPES value chain:
  - Generators, DSOs, TSOs, aggregators, prosumers
- Challenges
  - OT and IT integration and testing
  - A wide area of technologies used to develop the components
  - Different business aspects of the functionality (from behaviour analysis to anomaly detection and monitoring)

OUTCOMES ACHIEVED

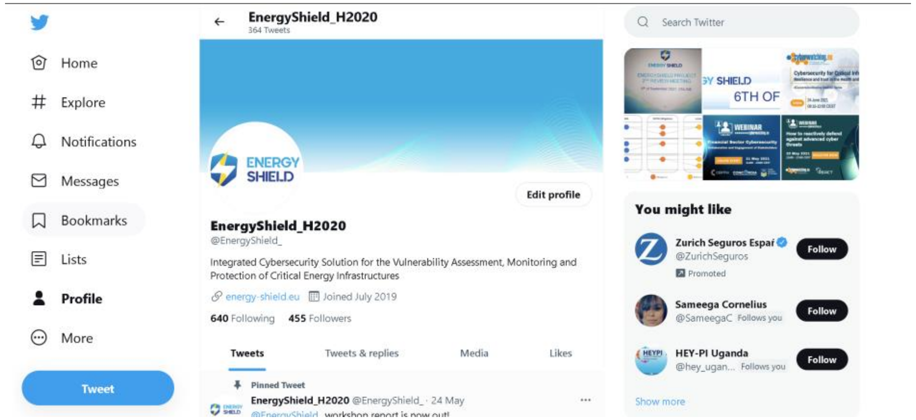
- the technology providers have improved and adapted the tools making them ready for integration through the overall EnergyShield system and interacted with Practitioners to collect feedback (testing and evaluation of tools
- a flexible integration concept was designed and is being implemented to ease the accommodation of tools a Portal to securely access the toolkit.
- technology providers have collaborated towards preparing and accommodating tools using different technologies in a common environment (EnergyShield toolkit) and using a data fusion mechanism combined machine learning to create a global view.

ONLINE PRESENCE

- Social media
  - Twitter
  - LinkedIn
- Project website
  - Articles on events participation
  - Newsletters
- 19 scientific articles published
- Foundation members in 2 clusters: CyberEPES and ESCI

SCAN ME

SCAN ME



EnergyShield_H2020
364 Tweets

EnergyShield_H2020
@EnergyShield_

Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

energy-shield.eu Joined July 2019

640 Following 455 Followers

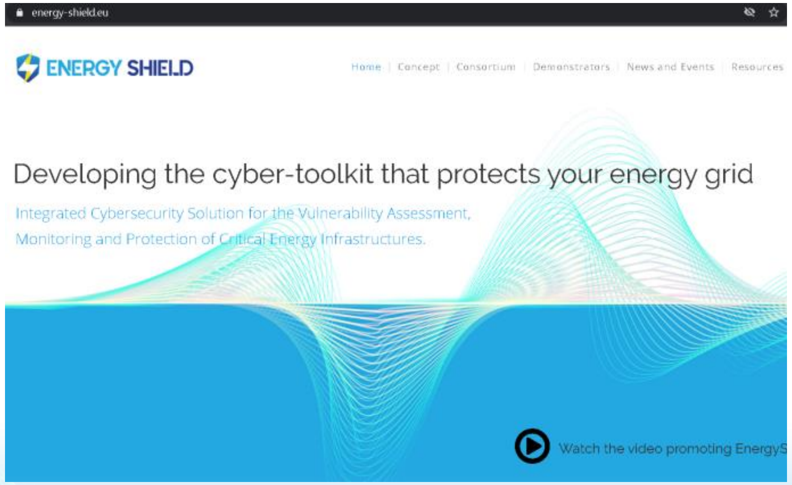
Pinned Tweet
EnergyShield_H2020 @EnergyShield_ · 24 May
@EnergyShield_ workshop report is now out!

You might like

Zurich Seguros Españ @ZurichSeguros Promoted

Sameega Cornelius @SameegaC Follows you

HEY-PI Uganda @hey_ugan... Follows you


energy-shield.eu
ENERGY SHIELD
Home | Concept | Consortium | Demonstrators | News and Events | Resources

Developing the cyber-toolkit that protects your energy grid

Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures.

Watch the video promoting EnergyS

COLLABORATION LANDSCAPE

SPHINX

HONOR

UNITED GRID

FLEXGRID

flexitranstore

PHOENIX

CYBERKIT 4SME

bridge HORIZON 2020

cyberwatching.eu The European watch on cybersecurity & privacy

ReachOut!

SDN-μSense

FARCROSS

erncip

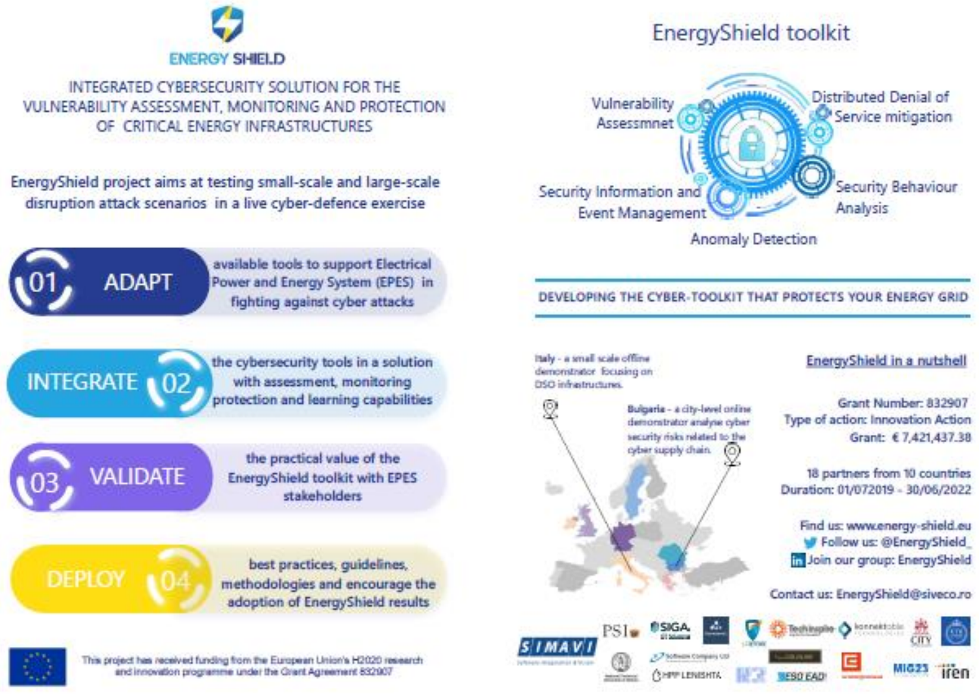
SPEAR

[Cybersecurity Innovation Cluster for EPES]

[ESCI Cluster]

REACH OUT THE PROJECT

- Find us: www.energy-shield.eu
- Subscribe for Newsletter
- Follow us: @EnergyShield_
- Join our LinkedIn group: EnergyShield
- Contact us: EnergyShield@siveco.ro
- Video presentation: https://youtu.be/AtSUmkrp1Dw
- Project Coordinator: SIMAVI
  - Otilia Bularca, Project Manager
  - E-mail: otilia.bularca@simavi.ro



ENERGY SHIELD

INTEGRATED CYBERSECURITY SOLUTION FOR THE VULNERABILITY ASSESSMENT, MONITORING AND PROTECTION OF CRITICAL ENERGY INFRASTRUCTURES

EnergyShield project aims at testing small-scale and large-scale disruption attack scenarios in a live cyber-defence exercise

01 ADAPT available tools to support Electrical Power and Energy System (EPES) in fighting against cyber attacks

INTEGRATE 02 the cybersecurity tools in a solution with assessment, monitoring protection and learning capabilities

03 VALIDATE the practical value of the EnergyShield toolkit with EPES stakeholders

DEPLOY 04 best practices, guidelines, methodologies and encourage the adoption of EnergyShield results

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement 832907

EnergyShield toolkit

Vulnerability Assessmnet
Distributed Denial of Service mitigation
Security Information and Event Management
Security Behaviour Analysis
Anomaly Detection

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

Italy - a small scale offline demonstrator focusing on DSO infrastructures.
Bulgaria - a city-level online demonstrator analyse cyber security risks related to the cyber supply chain.

EnergyShield in a nutshell

Grant Number: 832907
Type of action: Innovation Action
Grant: € 7,421,437.38

18 partners from 10 countries
Duration: 01/072019 - 30/06/2022

Find us: www.energy-shield.eu
Follow us: @EnergyShield_
Join our group: EnergyShield

Contact us: EnergyShield@siveco.ro

LESSONS LEARNED

- **Supply chains for components of critical infrastructure have gotten recently large attention of policy maker** in the telecommunication, especially on 5G-driver regulation and the market share targeted by global player.
  - This discussion is highly relevant for the energy sector as similar companies are also leading the sector of photovoltaic inverters.
- **Software supply chain risks became additionally very visible** after hackers inserted malware into the SolarWinds software, which was rolled-out to many customers from the government and critical infrastructure sector.
- Starting from a **plethora of technologies** and use case functionalities the EnergyShield system needs to provide full flexibility.
  - In this case monolith architecture is not feasible as limits the deployment possibilities, is difficult to scale and limits the adoption of new technologies.
  - Thus, to ease the deployment on a variety of system uncouples **containerization** is proposed.
- The market and competition assessment confirmed that many tools are cross sectors tools (i.e., no specific offer to the energy sector).
  - There have been **several recent incidents that provide good arguments for the exploitation of the EnergyShield toolkit**
    - the global SolarWinds incident (software supply chain attack), vulnerabilities in Microsoft Exchange and recently the attack to the Colonial Pipeline (USA).
  - on a high level, suppliers and customers agree that cybersecurity is important, but it is a completely different story to convince **utilities to install new cybersecurity (not established) devices into their critical infrastructures**
- Early establishment of a communication network is important for reaching our relevant stakeholders, creating synergies and facilitating cross-fertilization of similar projects.

ENERGY SHIELD

THANK YOU!

SIMAVI
Software Imagination & Vision

PSI

SIGA
OT Solutions

foreseeti

L7DEFENSE

РАЗПРЕДЕЛЕНИЕ

CITY
UNIVERSITY OF LONDON
EST 1894

KTH
VETENSKAP
OCH KONST

ΕΘΝ. ΜΕΤΣΟΒ. ΠΟΛΥΤΕΧΝΕΙΟΝ

ESO EAD

MIG23
turnkey engineering

TechInspire
Inspire for innovation

iren

GOLDLINE

HPP LENISHTA

SC Software Company Ltd
Developing quality software solutions since 1996

konnektable
TECHNOLOGIES

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 832907